

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG(19) Weltorganisation für geistiges Eigentum
Internationales Büro(43) Internationales Veröffentlichungsdatum
12. Februar 2004 (12.02.2004)

PCT

(10) Internationale Veröffentlichungsnummer
WO 2004/014040 A1(51) Internationale Patentklassifikation⁷: **H04L 29/06**

(21) Internationales Aktenzeichen: PCT/IB2003/002978

(22) Internationales Anmeldedatum:
25. Juli 2003 (25.07.2003)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
102 34 643.7 29. Juli 2002 (29.07.2002) DE(71) Anmelder (nur für DE): **PHILIPS INTELLECTUAL
PROPERTY & STANDARDS GMBH** [DE/DE]; Stein-
damm 94, 20099 Hamburg (DE).(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von
DE, US): **KONINKLIJKE PHILIPS ELECTRONICS
N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eind-
hoven (NL).

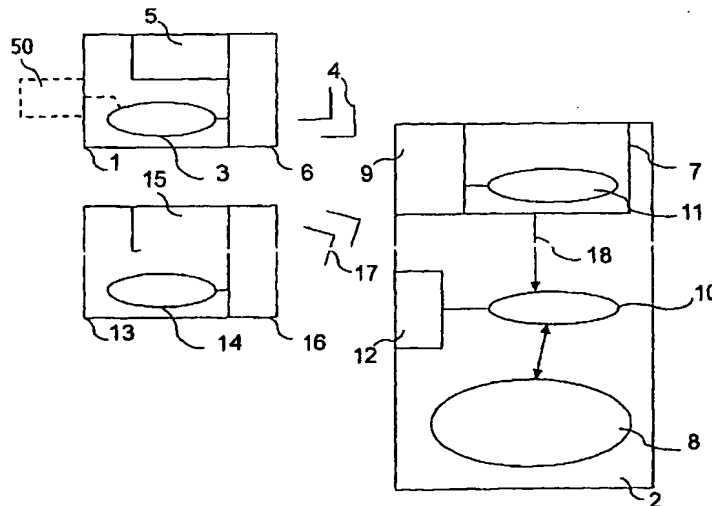
(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): **BUDDE, Wolfgang,
Otto** [DE/DE]; Philips Intellectual Property & Stan-
dards GmbH, Weisshausstr. 2, 52066 Aachen (DE).
SCHREYER, Oliver [DE/DE]; Philips Intellectual Prop-
erty & Standards GmbH, Weisshausstr. 2, 52066 Aachen
(DE). **LELKENS, Armand** [NL/DE]; Philips Intellectual
Property & Standards GmbH, Weisshausstr. 2, 52066
Aachen (DE). **ERDMANN, Bozena** [PL/DE]; Philips
Intellectual Property & Standards GmbH, Weisshausstr. 2,
52066 Aachen (DE).(74) Anwalt: **VOLMER, Georg**; Philips Intellectual Property
& Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

[Fortsetzung auf der nächsten Seite]

(54) Title: SECURITY SYSTEM FOR DEVICES OF A WIRELESS NETWORK

(54) Bezeichnung: SICHERHEITSSYSTEM FÜR GERÄTE EINES DRAHTLOSEN NETZWERKS



(57) Abstract: The invention relates to a security system for wireless networks. Said system comprises a first portable unit, which contains a memory (3) for storing a universally unambiguous key data record (4) and is designed to transmit the key data record (4) over short distances. A receiving device (7), which comprises a receiver (9) for receiving the key data record (4) and an evaluation component (11) for storing, processing and/or forwarding the key data record (4) or part of the key data record to a second component, is provided in at least one wireless device (2) of the network. The devices of the wireless network acquire a common secret key by means of the key data record, said key enabling the encoding and decoding of the transmitted useful data and/or authentication. According to an optional embodiment of the invention, the key data record can be derived from the biometric characteristics of a user and entered in the portable unit.

[Fortsetzung auf der nächsten Seite]



(81) **Bestimmungsstaaten (national):** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Bestimmungsstaaten (regional):** ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ,

TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— mit internationalem Recherchenbericht

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) **Zusammenfassung:** Die Erfindung bezieht sich auf ein Sicherheitssystem für drahtlose Netzwerke mit einer ersten tragbaren Einheit (1) mit einem Speicher (3) zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes (4), die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4) vorgesehen ist. In wenigstens einem drahtlosen Gerät (2) des Netzwerks ist eine Empfangseinheit (7) vorgesehen, die einen Empfänger (9) zum Empfang des Schlüsseldatensatzes (4) und eine Auswertekomponente (11) des Gerätes zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes (4) oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist. Durch den Schlüsseldatensatz erlangen die Geräte des drahtlosen Netzwerks einen gemeinsamen geheimen Schlüssel, mit Hilfe dessen die Ver- und Entschlüsselung der übertragenen Nutzdaten und/oder die Authentifizierung vorgenommen wird. Gemäß einer optionalen Ausgestaltung der Erfindung kann der Schlüsseldatensatz in die tragbare Einheit aus biometrischen Charakteristika eines Benutzers abgeleitet werden.

Sicherheitssystem für Geräte eines drahtlosen Netzwerks

5

Die vorliegende Erfindung bezieht sich allgemein auf ein Sicherheitssystem für drahtlose Netzwerke.

Der Einsatz von drahtloser Kommunikation zur Unterstützung mobiler Geräte (wie Schnurlostelefone) oder als Ersatz für drahtgebundene Lösungen zwischen stationären Geräten (z. B. PC und Telefonanschlussdose) ist schon heute weit verbreitet.

Für zukünftige digitale Hausnetzwerke bedeutet das, dass sie typischerweise nicht nur aus mehreren drahtgebundenen Geräten, sondern auch aus mehreren drahtlosen Geräten bestehen. Bei der Realisierung digitaler drahtloser Netzwerke, insbesondere Hausnetzwerke, werden Funktechnologien wie Bluetooth, DECT und vor allem der IEEE802.11 Standard für "Wireless Local Area Network" verwendet. Drahtlose Kommunikation kann auch über Infrarot (IrDA) erfolgen.

Desgleichen werden auch andere der Information oder Unterhaltung der Nutzer dienende Netze zukünftig unter anderem auch drahtlos kommunizierende Geräte enthalten. Insbesondere seien hier sogenannte Ad-hoc-Netzwerke genannt, bei denen es sich um temporär eingerichtete Netzwerke mit im Allgemeinen Geräten verschiedener Besitzer handelt. Ein Beispiel solcher Ad-hoc-Netzwerke findet sich in Hotels: ein Gast wird z. B. die Musikstücke auf seinem mitgebrachten MP3-Spieler über die Stereoanlage des Hotelzimmers wiedergeben wollen. Ein weiteres Beispiel sind alle Arten von Treffen, bei denen sich Menschen mit drahtlos kommunizierenden Geräten zum Austausch von Daten oder Medieninhalten (Bilder, Filme, Musik) zusammen finden.

Bei Verwendung von Funktechnologien können Geräte wie z.B. ein MP3-Speicher-Gerät und eine HiFi-Anlage drahtlos über Funkwellen als Datenleitung miteinander kommunizieren. Prinzipiell gibt es dabei zwei Betriebsarten. Entweder kommunizieren die Geräte direkt von Gerät zu Gerät (als Peer-to-Peer-Netzwerk) oder über einen zentralen Zugangspunkt (Access Point) als Verteilerstation.

Je nach Standard haben die Funktechnologien Reichweiten von mehreren

10 Metern in Gebäuden (IEEE802.11 bis zu 30m) und mehreren 100 Metern im Freien (IEEE802.11 bis zu 300m). Funkwellen durchdringen auch die Wände einer Wohnung oder eines Hauses. Im Abdeckungsbereich eines Funknetzes, also innerhalb der Reichweite können die übertragenen Informationen prinzipiell von jedem Empfänger, 5 der mit einer entsprechenden Funkschnittstelle ausgerüstet ist, empfangen werden.

Daraus ergibt sich die Notwendigkeit, drahtlose Netzwerke gegen unbefugtes oder auch unbeabsichtigtes Abhören der übertragenen Informationen, sowie gegen unbefugten Zugang zum Netzwerk und damit zu dessen Ressourcen besonders zu schützen.

10 Des Weiteren muss für ein Gerät, das sich in ein bestimmtes von mehreren innerhalb der Funkreichweite liegenden Netzen neu assoziieren will, eine eindeutige Identifikation des Zielnetzwerkes möglich sein.

Methoden zur Zugangskontrolle und zum Schutz der übertragenen Informationen sind in den Funkstandards enthalten (z.B. bei IEEE802.11 in " 15 IEEE802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Standard, IEEE", New York, August 1999, Kapitel 8). Allgemein in Funknetzen als auch speziell im IEEE802.11 Standard beruht jede Form der Datensicherheit letztlich auf geheimen Verschlüsselungscodes (Schlüsseln) oder Kennworten, die nur den befugten Kommunikationspartnern bekannt sind.

20 Zugangskontrolle bedeutet, zwischen befugten und unbefugten Geräten unterscheiden zu können, d.h. ein Zugang gewährendes Gerät (z.B. ein Access Point, oder ein Gerät eines Heim- oder Ad-hoc-Netzwerks, das eine Kommunikationsanforderung erhält) kann anhand von übermittelten Informationen entscheiden, ob ein Zugang forderndes Gerät befugt ist. Bei einem Medium wie Funk, 25 das leicht abgehört werden kann, ist dabei die einfache Übertragung von Zugangscodes oder die Verwendung von Identifikatoren (die vom Zugang gewährenden Gerät mit einer Liste von Identifikatoren befugter Geräte verglichen werden kann) unzureichend, da ein unbefugtes Gerät durch Mithören dieser Übertragung unberechtigt an die notwendigen Zugangsinformationen gelangen kann.

30 Das in Zusammenhang mit IEEE802.11 verwendete sogenannte MAC-Address-Filtering stellt in seiner einfachen Form keinen sicheren Schutz dar. Bei dieser Methode speichert der Access Point die Liste der MAC (Media Access Control)-

Adressen der zum Zugriff auf das Netzwerk befugten Geräte. Versucht ein unbefugtes Gerät auf das Netzwerk zuzugreifen, wird es aufgrund der dem Access Point unbekannten MAC-Adresse zurückgewiesen. Neben der für Hausnetzwerke inakzeptablen Benutzerunfreundlichkeit der notwendigen Wartung einer MAC-

- 5 Adressen-Liste hat diese Methode vor allem den Nachteil, dass es möglich ist, MAC-Adressen vorzutäuschen. Somit muss es einem unbefugten Benutzer nur gelingen, Kenntnis einer "befugten" MAC-Adresse zu erhalten, was wiederum beim Belauschen des Funkverkehrs einfach möglich ist. Deshalb wird Zugangskontrolle mit einer Authentifizierung gekoppelt, die auf einem geheimen Schlüssel oder Kennwort beruht.

- 10 Im IEEE802.11 Standard ist die "Shared-Key-Authentifizierung" definiert, bei der sich ein befugtes Gerät durch die Kenntnis eines geheimen Schlüssels auszeichnet. Die Authentifizierung wird dann wie folgt vorgenommen: Um die Befugnis festzustellen, sendet das Zugang gewährende Gerät einen Zufallswert (Challenge), den das Zugang fordernde Gerät mit dem geheimen Schlüssel verschlüsselt
15 und zurücksendet. Dadurch kann das Zugang gewährende Gerät die Kenntnis des Schlüssels und damit die Zugangsberechtigung verifizieren (diese Methode wird in seiner allgemeinen Form auch "Challenge-Response-Methode" genannt).

- Bei der Verschlüsselung werden die übertragenen Informationen vom sendenden Gerät verschlüsselt und vom empfangenden Gerät entschlüsselt, so dass die
20 Daten für einen unbefugten oder unbeabsichtigt Mithörenden wertlos sind. Der IEEE802.11 Standard verwendet dazu die Verschlüsselungsmethode Wired Equivalent Privacy (WEP). Dabei wird ein allen Geräten des Netzwerks bekannter, aber sonst geheimer Schlüssel (40 Bit oder 104 Bit WEP-Schlüssel) verwendet, der als Parameter in den im IEEE802.11 Standard festgelegten Verschlüsselungsalgorithmus zur
25 Verschlüsselung der zu übertragenden Daten eingeht.

Im Falle von WEP wird derselbe Schlüssel auch zur Authentifizierung verwendet.

- Neben "symmetrischen" Verschlüsselungsverfahren (mit einem "shared key") gibt es auch die sogenannten public/private key-Verfahren, bei denen jedes Gerät
30 einen allgemein bekannten Schlüssel (public key) zum Verschlüsseln bereit stellt und einen dazugehörigen, nur diesem Gerät bekannten geheimen Schlüssel (private key) besitzt, der das Entschlüsseln der mit dem public key verschlüsselten Informationen

ermöglicht.

Dadurch ist Abhörsicherheit ohne einen im Voraus bekannten gemeinsamen geheimen Schlüssel möglich. Bei Anwendung dieser Art von Verfahren ist es jedoch einem beliebigen Gerät möglich, unter Nutzung des allgemein bekannten

5 Schlüssels die Kommunikation zu einem Gerät (z.B. einem Zugang gewährenden Gerät) aufzunehmen. Deshalb ist auch hier eine Authentifizierung zur Zugangskontrolle notwendig, die wiederum auf einem geheimen Schlüssel beruht, der im Voraus den Kommunikationspartnern bekannt sein muss.

Zur Erhöhung der Datensicherheit können Netzwerkgeräte Mechanismen

10 zur Vereinbarung von temporären Schlüsseln beinhalten, also Schlüsseln, die nur eine festgelegte Zeitspanne lang zur Verschlüsselung verwendet werden, so dass nicht immer derselbe geheime Schlüssel verwendet wird. Der Austausch dieser temporären Schlüssel erfordert aber eine abhörsichere Übertragung, die wiederum zumindest einen ersten geheimen Schlüssel benötigt, der im Voraus den Kommunikationspartnern bekannt sein muss.

15 muss. Wesentlich für die Erfindung ist, dass auch die Datensicherheit durch Verschlüsselung auf einem (ersten) geheimen Schlüssel beruht, der im Voraus den Kommunikationspartnern bekannt sein muss.

Um ein Sicherheitssystem für drahtlose Netzwerke zu schaffen, ist deshalb ein Konfigurationsschritt notwendig, der allen relevanten Geräten einen

20 geheimen Schlüssel (für Authentifizierung und/oder Verschlüsselung) zur Verfügung stellt.

Dabei ist eine Besonderheit drahtloser Netzwerke, dass dieser Schlüssel nicht als "Klartext" (unverschlüsselt) über die drahtlose Kommunikationsschnittstelle übertragen werden sollte, da sonst ein unbefugtes Gerät durch mithören unberechtigt an

25 den Schlüssel gelangen kann. Zwar kann durch Kodiervorgahren, wie Diffie-Hellman, die abhörsichere Vereinbarung eines gemeinsamen geheimen Schlüssels zwischen zwei Kommunikationspartnern über eine Funkschnittstelle erreicht werden. Um jedoch zu verhindern, dass ein unbefugtes Gerät die Schlüsselvereinbarung mit einem (Zugang gewährenden) Gerät des Netzwerkes initiiert, muss auch dieses Verfahren mit einer

30 Authentifizierung der Kommunikationspartner gekoppelt sein, was wiederum einen (ersten) geheimen Schlüssel erfordert, der im Voraus den Kommunikationspartnern bekannt sein muss.

Bei Schnurlostelefonen nach DECT-Standard ist ein erster Schlüssel bereits ab Werk in den Geräten (Basisstation und Hörer) gespeichert. Zur Anmeldung eines neuen Hörers an der Basisstation muss der Schlüssel (PIN-Nummer), der in der Basisstation gespeichert ist, vom Benutzer am neuen Hörer eingegeben werden. Da der Benutzer den Schlüssel dazu kennen muss, ist dieser z.B. auf Aufklebern an der Basisstation verfügbar.

IEEE 802.11 basierte Firmen- oder Campus-Netzwerke mit einer dedizierten Infrastruktur werden im allgemeinen von speziell ausgebildeten Systemadministratoren konfiguriert. Diese benutzen im allgemeinen System-Management-Rechner, die drahtgebundene Verbindungen zu jedem Access Point besitzen. Über diese drahtgebundenen (und damit quasi abhörsicheren) Verbindungen werden die geheimen Schlüssel (z.B. WEP-Schlüssel) zu den Access Points übertragen. Die Schlüsseleingabe an den Klienten (z.B. drahtlose Laptops) erfolgt von Hand.

Die Durchführung eines Konfigurationsschrittes zur Installation eines ersten geheimen Schlüssels wird zwar vorausgesetzt (und die notwendigen Konfigurationsschritte sind in Software-Schnittstellen definiert), aber die Realisierung ist nicht festgelegt. Der IEEE802.11 Standard beinhaltet dazu in Kapitel 8.1.2 folgendes Statement: "The required secret shared key is presumed to have been delivered to participating STAs (stations) via a secure channel that is independent of IEEE 802.11. The shared key is contained in a write only MIB (Management Information Base) attribute via the MAC management path."

Die Durchführung eines Konfigurationsschrittes zur Installation eines ersten (geheim gehaltenen oder nicht geheim gehaltenen) Schlüssels als Netzzidentifikator ist auch eine generelle Voraussetzung für eine automatisierte Konfiguration drahtloser Netzwerke, da sonst ein Gerät (falls funktechnisch in der Reichweite mehrere Netze, z.B. der Nachbarwohnung) nicht entscheiden kann, zu welchem Netzwerk es assoziieren soll.

Der Erfindung liegt die Aufgabe zugrunde, eine benutzerfreundliche Installation eines (vorzugsweise geheimen) Schlüssels in den Geräten eines drahtlosen Netzwerks zu realisieren.

Die Aufgabe wird gelöst durch ein Sicherheitssystem für drahtlose Netzwerke ausgestattet mit

einer ersten tragbaren Einheit mit einem Speicher zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes, die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes vorgesehen ist, und mindestens einer Empfangseinheit in wenigstens einem drahtlosen Gerät des Netzwerks, die einen Empfänger zum Empfang des Schlüsseldatensatzes und eine Auswertekomponente des Gerätes zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist.

Jedes drahtlose Gerät des Netzwerks hat sowohl eine Funkschnittstelle zum Übertragen von Nutzdaten als auch eine Empfangseinheit zum Empfang eines Schlüsseldatensatzes von einer ersten tragbaren Einheit. Zur Sicherung des drahtlosen Nutzdatenverkehrs zwischen den Geräten wird in jedes Gerät abhörsicher ein Schlüsseldatensatz eingegeben, durch den diese Geräte einen gemeinsamen geheimen Schlüssel erlangen, mit Hilfe dessen die Ver- und Entschlüsselung der übertragenen Nutzdaten und/oder die Authentifizierung vorgenommen wird.

Zusätzlich oder alternativ kann der Schlüsseldatensatz zur Netzwerk-Identifikation verwendet werden, d.h. um einem neuen Gerät die Einkopplung in das "richtige" Netzwerk zu ermöglichen.

Der Schlüsseldatensatz ist im Speicher der tragbaren Einheit gespeichert, die über einen Sender oder einen Sender mit Detektoreinheit zur Kurzstreckenübertragung verfügt. Damit wird der Schlüsseldatensatz abhörsicher in jedes drahtlose Gerät des Netzwerkes eingegeben. Zur Auslösung einer Schlüsseldatensatzübertragung kann eine Taste an der Einheit dienen. Abhängig von dem verwendeten Verfahren zur Kurzstreckeninformationsübertragung kann die Auslösung einer Schlüsseldatensatzübertragung aber auch dadurch erfolgen, dass die Einheit in unmittelbare Nähe der Empfangseinheit gebracht wird und die Detektoreinheit die Schlüsseldatensatzübertragung auslöst.

Der Schlüsseldatensatz enthält als wesentlichen (und möglicherweise einzigen) Bestandteil einen geheimen Schlüsselcode ("Schlüssel"). Zum Empfang des Schlüsseldatensatzes verfügt jedes drahtlose Gerät des Netzwerkes über eine Empfangseinheit bestehend aus einem Empfänger und einer Auswertekomponente, die nach Erhalt des Schlüsseldatensatzes den Schlüssel extrahiert und diesen über eine

interne Schnittstelle an die für die Ver- und Entschlüsselung der Nutzdaten zuständige zweite Komponente (z.B. die für die Steuerung der Funkschnittstelle zuständige Treibersoftware) weiterleitet.

Ein durch die tragbare Einheit verwendetes Verfahren zur

- 5 Kurzstreckeninformationsübertragung kann auf modulierten magnetischen-, elektromagnetischen Feldern, sowie Infrarot- oder sichtbarem Licht, Ultra- oder Infraschall oder beliebigen anderen, in ihrer Reichweite kontrollierbaren Übertragungstechnologien basieren. Die Übertragung des Schlüsseldatensatzes kann auch durch ein mehrdimensionales Muster auf der Oberfläche des Senders realisiert
- 10 werden, welches von der Empfangseinheit ausgelesen wird. Wesentlich für die Erfindung ist, dass eine Technologie mit sehr kurzer Reichweite (wenige Zentimeter) oder kurzer Reichweite und starker lokaler Begrenzung (z.B. Infrarot) benutzt wird, so dass die Eingabe der Schlüsseldatensatz aus einer sehr kurzen Distanz stattfindet und auf keinen Fall die Wände eines Raumes durchdringen kann.

- 15 Ein besonderer Vorteil dieser Lösung besteht darin, dass Unbefugten der Empfang des Schlüsseldatensatzes nicht möglich ist. Die Übertragung des Schlüsseldatensatzes kann durch einen Tastendruck an der tragbaren Einheit ausgelöst werden oder - z.B. bei Verwendung von Hochfrequenz-Transpondertechnologie (kontaktloser RF-tag Technologie) - auch dadurch, dass die tragbare Einheit in
- 20 unmittelbarer Nähe der Empfangseinheit platziert wird. Somit ist das Eingeben des Schlüsseldatensatzes in ein Gerät für einen Benutzer durch Annähern der tragbaren Einheit an das Gerät (oder Richten der Einheit auf das Gerät) und eventuelles Betätigen einer Taste an der Einheit besonders einfach und unkompliziert. Der Benutzer benötigt auch keine Kenntnis über den Inhalt des Schlüsseldatensatzes bzw. den geheimen
- 25 Schlüssel. Ein Fachmann für die Eingabe und die Administration des Schlüsseldatensatzes ist nicht notwendig. Die Benutzerfreundlichkeit ist ein weiterer besonderer Vorteil dieser Lösung.

Der Schlüsseldatensatz der tragbaren Einheit kann beispielsweise vom Hersteller vorgegeben und dauerhaft im Speicher der Einheit abgespeichert werden.

- 30 Gemäß einer Weiterbildung der Erfindung weist die tragbare Einheit indes eine Eingabevorrichtung auf, über welche ein Benutzer einen Schlüsseldatensatz in den Speicher eingeben kann. Im einfachsten Falle kann es sich bei der Eingabe-

vorrichtung um eine Tastatur handeln, über welche der Benutzer einen Code als Schlüsseldatensatz eingeben kann. Ebenso kann die Eingabevorrichtung jedoch auch eine Spracherkennungseinheit sein, welche aus vorgesprochenen Worten bzw. Sätzen (unabhängig von der Identität des Sprechers) ein Passwort ableitet und im Speicher
5 hinterlegt.

Weiterhin kann die Eingabevorrichtung dazu eingerichtet sein, biometrische Charakteristika eines Benutzers zu erfassen und aus diesen einen Schlüsseldatensatz abzuleiten. Die Ableitung eines Schlüsseldatensatzes aus biometrischen Charakteristika eines Benutzers stellt sicher, dass der Schlüsseldatensatz
10 weltweit eindeutig ist.

Bei der über eine Eingabevorrichtung vorgenommenen Bereitstellung eines Schlüsseldatensatzes (per expliziter Eingabe, Erfassung biometrischer Charakteristika oder dergleichen) ist die tragbare Einheit vorzugsweise zusätzlich dazu eingerichtet, den genannten Schlüsseldatensatz (einschließlich aller hiermit korrelierten
15 Daten) nach einer vorgegebenen Zeitdauer von zum Beispiel 30 Sekunden und/oder nach einer vorgegebenen Verarbeitungsprozedur, zum Beispiel der Übertragung des Schlüsseldatensatzes an ein Gerät eines Netzwerkes, wieder aus dem Speicher der tragbaren Einheit zu löschen. Dies bedeutet, dass der Schlüsseldatensatz nicht auf Dauer in der tragbaren Einheit gespeichert wird, sodass ein Besitz der Einheit in der Regel
20 keinen Missbrauch des Schlüsseldatensatzes ermöglicht. Der berechtigte Benutzer muss vielmehr bei jeder Verwendung der tragbaren Einheit erneut den Schlüsseldatensatz eingeben. Eine besonders sichere Verwahrung der tragbaren Einheit ist daher nicht erforderlich, was es wiederum ermöglicht, die Einheit in vielen gängigen Geräten zu integrieren. Beispielsweise könnte sie Teil einer Fernsteuerung (z.B. iPronto, Philips),
25 eines Mobiltelefons, eines USB-Dongles etc. sein.

Drahtlose Netzwerke, insbesondere Hausnetzwerke, sollten Zugriff nicht nur für ständige Benutzer des Hausnetzwerks (z.B. Eigentümer) bieten, sondern auch einen ggf. beschränkten Zugriff für temporäre Benutzer wie z.B. Gäste ermöglichen.

Eine vorteilhafte Weiterbildung der Erfindung besteht aus einer als
30 Schlüsselgenerator bezeichneten Komponente, die zur Erzeugung zusätzlicher Schlüsseldatensätze dient. Der Schlüsselgenerator ist eine zusätzliche Komponente der ersten tragbaren Einheit oder in einer zweiten separaten tragbaren Einheit realisiert.

Ein vom Schlüsselgenerator erzeugter Schlüsseldatensatz, sog. Gast-Schlüsseldatensatz, ist so aufgebaut, dass er immer (z.B. durch spezielle Bits im Schlüsseldatensatz) von einem im Speicher der Einheit gespeicherten (Heim-)Schlüsseldatensatz unterschieden werden kann. Ebenso ist bei einer Eingabe eines

5 Schlüsseldatensatzes immer klar, ob ein Heim-Schlüsseldatensatz oder ein Gast-Schlüsseldatensatz eingegeben wird. Dazu hat die tragbare Einheit mit Speicher und Schlüsselgenerator mindestens zwei Tasten (eine, um die Übertragung des Heim-Schlüsseldatensatzes aus dem Speicher auszulösen und eine, um die Übertragung eines Gast-Schlüsseldatensatzes auszulösen). Ist der Schlüsselgenerator in einer separaten

10 zweiten Einheit realisiert, so ist diese eindeutig (z.B. durch Farbe, Aufschrift etc.) von der Einheit mit dem Heim-Schlüsseldatensatz unterscheidbar.

Ein Gast-Schlüsseldatensatz wird benutzt, um Gästen Zugriff auf Ressourcen des Netzwerks zu gewähren. Dazu wird an allen betreffenden (das heißt für die Nutzung in Verbindung mit den Geräten des Gastes freigegebenen) Geräten des

15 Hausnetzwerks und den Geräten des Gastes (die nicht zum Hausnetzwerk gehören) ein Gast-Schlüsseldatensatz eingegeben, mit Hilfe dessen die Geräte des Gastes (z.B. Laptop) mit den betreffenden Geräten des Hausnetzwerks kommunizieren können. In einer alternativen Ausprägung wird der Gastschlüsseldatensatz dem Netzwerk einmal bekanntgegeben (z.B. durch Eingeben in eines der zum Netzwerk gehörigen Geräte) und

20 braucht dann bei Bedarf nur noch in die Geräte des Gastes eingegeben zu werden; damit sind dann alle Geräte des Netzwerks für die Benutzung mit den Geräten des Gastes freigegeben. Die Steuerung, auf welche Daten innerhalb der freigegebenen Geräte der Gast Zugriff haben soll, muss an anderer Stelle erfolgen.

Um dem Benutzer die Kontrolle über die Dauer des gewährten Gast-

25 Zugangs zum Hausnetz zu ermöglichen, wird automatisch nach einer festgelegten Zeitspanne oder durch Benutzer-Interaktion der Gast-Schlüsseldatensatz in den Geräten des Hausnetzwerks gelöscht. Eine Benutzer-Interaktion zur Löschung eines Gast-Schlüsseldatensatzes kann z.B. die nochmalige Eingabe des aktuellen Heim-Schlüsseldatensatzes, ein spezieller Tastendruck an den betroffenen Hausnetz-Geräten oder an

30 einem der betroffenen Hausnetz-Geräte und nachfolgende automatische Information aller anderen betroffenen Hausnetz-Geräte durch dieses Gerät sein.

Um eine unbefugte Benutzung eines Gast-Schlüsseldatensatzes durch

einen früheren Gast zu verhindern, erzeugt der Schlüsselgenerator nach einer festgelegten Zeitspanne (z.B. 60 Minuten) nach der letzten Gast-Schlüsseldatensatzübertragung automatisch einen neuen Gast-Schlüsseldatensatz nach dem Zufallsprinzip. Dadurch erhält ein neuer Gast einen anderen Gast-

5 Schlüsseldatensatz als der vorherige, wodurch sichergestellt ist, dass der vorherige Gast die Anwesenheit des neuen Gastes nicht zum unbefugten Zugang zum Hausnetz ausnutzen kann.

Ad-hoc-Netzwerke stellen eine weitere Ausprägung drahtloser Netzwerke dar, in denen temporär eine Anzahl von Geräten zur Kommunikation in

10 einem gemeinsamen Netzwerk freigegeben werden sollen. In ähnlicher Weise wie beim Gastzugriff auf Hausnetzwerke, bei dem mittels eines Gast-Schlüsseldatensatzes einzelne Gast-Geräte für den Zugriff auf das Hausnetzwerk freigegeben werden, sollen beim Ad-hoc-Netzwerk Geräte anderer Besitzer mit mindestens einem Gerät des Benutzers kommunizieren können. Dazu gibt der Benutzer einen Schlüsseldatensatz,

15 hier Ad-hoc-Schlüsseldatensatz genannt, in alle Geräte des Ad-hoc-Netzwerks (seine eigenen und die der anderen Benutzer) ein. Der Ad-hoc-Schlüsseldatensatz kann in einer Ausprägung ein Gast-Schlüsseldatensatz sein, er kann aber auch als Ad-hoc-Schlüsseldatensatz eindeutig gekennzeichnet sein.

Es ist bevorzugt, dass die Schlüsseldatensätze aus Bitfolgen bestehen,

20 wobei jede Bitfolge in einem vordefinierten Format (z.B. als 1024-Bit Sequenz) übertragen wird.

Die gesamte Bitfolge oder ein Teil davon wird von der Empfangseinheit als Schlüssel weitergeleitet. Falls die Bitfolge neben dem Schlüssel zusätzliche Bits beinhaltet, so ist genau festgelegt, welcher Teil der Bitfolge als Schlüssel verwendet

25 wird (z.B. die 128 low-order Bits) und welche Bits der Bitfolge welche zusätzlichen Informationen beinhalten. Weitere Informationen können dabei Kennzeichnungen sein, die über die Art des Schlüsseldatensatzes (Heim-, Gast- oder Ad-hoc-) informieren oder Angaben über die Länge und Anzahl der Schlüsselcodes enthalten, falls mehrere Schlüsselcodes gleichzeitig übertragen werden. Im Falle dass die Empfangseinheit für

30 weitere Anwendungen genutzt wird, kennzeichnen die zusätzlichen Bits auch die Verwendung der Bitfolge als Schlüsseldatensatz.

Damit in zwei benachbarten Hausnetzwerken nicht der gleiche (Heim-

)Schlüssel verwendet wird, sollte dieser global eindeutig sein. Dies kann erreicht werden z.B. indem verschiedene Einheiten-Hersteller unterschiedliche Wertebereiche von Schlüsselcodes benutzen und innerhalb dieser Bereiche so weit wie möglich in keinen zwei Einheiten den gleichen Schlüsseldatensatz speichern.

- 5 Weiterhin kann wie oben erläutert ein Schlüsseldatensatz auf der Basis biometrischer Charakteristika eines Benutzers erzeugt werden.

Ein nach dem IEEE802.11 Standard arbeitendes Netzwerk ist ein weit verbreitetes Beispiel für drahtlose Hausnetzwerke. In einem IEEE802.11 Netzwerk kann der zu übertragene Schlüsseldatensatz einen oder mehrere Wired Equivalent

- 10 Privacy (WEP) - Schlüssel enthalten.

Die Eingabe des (Heim-)Schlüsseldatensatzes kann auch in Schritten zur Konfiguration des Netzwerks stattfinden, so dass zu Beginn der Konfiguration die Eingabe/ Installation des Schlüsseldatensatzes verlangt wird. Dadurch ist während des gesamten Konfigurationsprozesses eine abhörsichere Kommunikation der Geräte

- 15 untereinander, sowie eine Zugangskontrolle (befugt sind alle Geräte, die über den Schlüsseldatensatz verfügen) gewährleistet. Darüber hinaus kann der Schlüssel auch zur Netzwerk-Identifikation verwendet werden. Dies ist insbesondere vorteilhaft bei der Anwendung automatisierter Konfigurationsverfahren, d.h. Verfahren ohne Benutzer-Interaktion (basierend auf Mechanismen wie z.B. IPv6 Auto-Konfiguration und

- 20 Universal Plug and Play (UPnP)).

In einer bevorzugten Ausführungsform ist die tragbare Einheit in eine Fernbedienung eines Gerätes des Hausnetzwerks integriert.

- 25 Die Erfindung betrifft auch eine tragbare Einheit zur Installation eines gemeinsamen Schlüssels in wenigstens einem Gerät eines drahtlosen Netzwerkes mit einem Speicher zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes, die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes vorgesehen ist.

- Weiterhin betrifft die Erfindung ein elektrisches Gerät mit einer Empfangseinheit, die einen Empfänger zum Empfang eines Schlüsseldatensatzes und eine Auswertekomponente des Gerätes zur Speicherung, Weiterleitung und/oder
- 30 Verarbeitung des Schlüsseldatensatzes oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist.

Ausführungsbeispiele der Erfindung werden nachstehend anhand der

Abbildung Fig.1 näher erläutert.

Es zeigen:

- 5 Fig. 1 eine schematische Darstellung zweier Einheiten und eines
Gerätes,
Fig. 2 Blockschaltbild einer Einheit als Sendeeinheit bei Verwendung
von Hochfrequenz-Transpondertechnologie,
Fig. 3 Blockschaltbild einer Einheit als Empfangs- und Sendeeinheit bei
10 Verwendung von Hochfrequenz-Transpondertechnologie, und
Fig. 4 Blockschaltbild einer Einheit als eine Gästeeinheit bei
Verwendung von Hochfrequenz-Transpondertechnologie

- 15 Anhand Fig. 1 wird die Installation eines elektrischen Gerätes in ein
Hausnetzwerk, das aus hier nicht dargestellten, drahtlosen und drahtgebundenen
Geräten besteht, beschrieben. Dargestellt sind eine erste, tragbare Einheit 1, eine
Gästeeinheit 13 und ein Personal-Computer (PC) 2 als ein im Hausnetzwerk neues
Gerät. Die drahtlosen Geräte des Hausnetzwerks besitzen alle entsprechende, am
20 Beispiel des PCs 2 beschriebene Komponenten 8 bis 12.

- Die erste Einheit 1 besteht aus einem Speicher 3 zur Speicherung eines
Schlüsseldatensatzes 4, einer ersten Taste 5 als eine Einheit zur Auslösung einer
Schlüsselübertragung und einem ersten Sender 6, der als eine drahtlose Schnittstelle
zum Aussenden des Schlüsseldatensatzes 4 dient. Die Einheit 1 zeichnet sich durch ihre
25 kurze Reichweite von maximal etwa 50 cm aus.

- Die Gästeeinheit 13 beinhaltet eine als Schlüsselgenerator 14 bezeichnete
Komponente zur Erzeugung von Schlüsseldatensätzen, z.B. nach dem Zufallsprinzip,
eine zweite Taste 15 und einen zweiten Sender 16. Die Gästeeinheit 13 ermöglicht
Gästen mit eigenen Geräten (die nicht zum Hausnetzwerk gehören) einen ggf. nur
30 beschränkten Zugriff auf die Geräte und Anwendungen des Hausnetzwerks. Deshalb
wird ein durch den Schlüsselgenerator 14 erzeugter Schlüsseldatensatz als Gast-
Schlüsseldatensatz 17 bezeichnet.

- Der PC 2 ist ein mit einer nach dem IEEE802.11-Standard arbeitenden Funkschnittstelle 12 ausgestattetes Gerät, dessen Funkschnittstelle 12 durch eine als Treibersoftware 10 bezeichnete Komponente kontrolliert wird und zur Übertragung von Nutzdaten (Musik, Video, allgemeine Daten, aber auch Steuerdaten) dient. Die
- 5 Treibersoftware 10 kann über standardisierte Softwareschnittstellen (APIs) von anderen Softwarekomponenten angesprochen werden. Zusätzlich ist der PC 2 mit einer Empfangseinheit 7 ausgestattet. Die Empfangseinheit 7 besteht aus einem Empfänger 9, der als Schnittstelle zum Empfang der von Sendern 6 oder 16 gesendeten Schlüsseldatensätze 4 oder 17 vorgesehen ist. In der Empfangseinheit 7 ist als
- 10 Auswertekomponente eine Empfängersoftware 11 vorgesehen, die nach Erhalt eines Schlüsseldatensatzes aus diesem einen Schlüssel 18 (z. B. einen in dem IEEE802.11 Standard definierten Wired Equivalent Privacy (WEP)-Schlüssel) extrahiert und diesen Schlüssel 18 über eine standardisierte Management-Schnittstelle (als MIB (Management Information Base) - Attribut beim IEEE802.11-Standard) an die Treibersoftware 10
- 15 weiterleitet. Der PC 2 weist eine zum Betrieb des PCs notwendige Anwendungssoftware 8 auf.

- Ein Benutzer möchte den PC 2 ins Hausnetzwerk installieren und drahtlos mit einer HiFi-Anlage des Hausnetzwerkes verbinden, damit er mehrere im PC 2 gespeicherte Musikdateien im MP3-Format auf seiner HiFi-Anlage abspielen kann.
- 20 Dazu begibt sich der Benutzer mit der Einheit 1 in die Nähe des PCs 2 und startet eine Übertragung des im Speicher 3 gespeicherten Schlüsseldatensatzes 4, indem er aus einer Entfernung von einigen Zentimetern den Sender 6 der Einheit 1 auf den Empfänger 9 richtet und die Taste 5 der Einheit 1 betätigt.

- Bei der Übertragung des Schlüsseldatensatzes 4 werden Infrarotsignale
- 25 verwendet. Das Format des Schlüsseldatensatzes 4 ist eine 1024 Bit-Sequenz, aus welcher die Empfängersoftware 11 die 128 low-order Bits extrahiert und als (WEP-)Schlüssel 18 an die Treibersoftware 10 weiterleitet. In der Treibersoftware 10 wird dieser Schlüssel 18 zur Verschlüsselung des Datenverkehrs zwischen dem PC 2 und der HiFi-Anlage sowie anderen Geräten, bei denen ebenfalls die Eingabe des
- 30 Schlüsseldatensatzes 4 stattgefunden hat, verwendet. Dies bezieht sich auch auf die nachfolgend zur Auto-Konfiguration der Netzwerkanbindung des PCs an das Hausnetz (z.B. Konfiguration einer IP-Adresse) notwendige Kommunikation mit den schon im

Netzwerk vorhandenen Geräten.

Verschiedene Umstände können die Installation eines neuen Schlüssels erfordern, z.B. wenn die Einheit dem Benutzer abhanden kommt, ein neues Gerät installiert werden soll oder wenn der Benutzer einen Verdacht hat, dass sein

- 5 Hausnetzwerk nicht mehr geschützt ist. Grundsätzlich kann eine neue Einheit mit einem neuen Schlüsseldatensatz den zuletzt eingegebenen (alten) Schlüsseldatensatz überschreiben, wobei dann der neue Schlüsseldatensatz an allen Geräten des Hausnetzwerks neu eingegeben werden muss.

- Ein missbräuchliches Eingeben eines neuen Schlüsseldatensatzes in das
- 10 Hausnetz kann dadurch verhindert werden, dass mindestens ein Gerät des Hausnetzes für unbefugte Personen nicht frei zugänglich ist. Dieses Gerät kann nach der unbefugten Eingabe des neuen Schlüsseldatensatzes in die anderen Geräte des Hausnetzes nicht mehr mit diesen kommunizieren und z.B. einen entsprechenden Alarm auslösen.

- Um die Sicherheit des Hausnetzwerks zu erhöhen, kann es aber auch
- 15 Vorschrift sein, dass zur Eingabe eines neuen Schlüsseldatensatzes die zusätzliche Eingabe des alten Schlüsseldatensatzes 4 erforderlich ist. Dazu begibt sich der Benutzer mit der alten und der neuen Einheit in die direkte Nähe des PCs 2 oder eines anderen Gerätes des Hausnetzwerks. Der Benutzer betätigt die Taste 5 der alten Einheit 1 zur (nochmaligen) Übertragung des alten Schlüsseldatensatzes 4. Kurz darauf startet der
- 20 Benutzer die Übertragung des neuen Schlüsseldatensatzes, indem er bei der neuen Einheit die Taste zur Auslösung der Übertragung betätigt.

- Die Empfängersoftware 11 des PCs 2 registriert den Empfang des alten Schlüsseldatensatzes 4 und empfängt danach den neuen Schlüsseldatensatz. Nur unter der Bedingung, dass die Empfängersoftware 11 zuvor den Empfang des alten Schlüssel-
- 25 datensatzes 4 registriert hat, leitet sie den neuen Schlüsseldatensatz bzw. den enthaltenen Schlüssel über die Management-Schnittstelle an die Treibersoftware 10 der Funkschnittstelle 12 weiter. Damit eine Verschlüsselung des Datenverkehrs auf Basis des neuen Schlüssels stattfinden kann, muss die oben beschriebene Eingabe des neuen Schlüsseldatensatzes an allen Geräten des Hausnetzwerks vorgenommen werden.

- 30 Ein erhöhtes Maß an Sicherheit bei der Eingabe eines neuen Schlüsseldatensatzes kann erzielt werden, wenn die Empfängersoftware 11 die Eingabe eines neuen Schlüsseldatensatzes nur akzeptiert, d.h. den enthaltenen Schlüssel

weiterleitet, wenn der neue Schlüsseldatensatz mehrfach und in gewissen zeitlichen Abständen in das Gerät eingegeben wird, wobei Anzahl und zeitlicher Abstand der geforderten Eingaben nur dem Benutzer bekannt sind.

Ein erhöhtes Maß an Sicherheit des Hausnetzes kann auch dadurch erzielt werden, dass ein Schlüsseldatensatz regelmäßig nach Ablauf einer gewissen Zeitspanne (mehrere Tage/Wochen/Monate) erneut an mindestens ein Gerät des Hausnetzes übertragen werden muss.

Bei der bis hierher erfolgenden Beschreibung der Erfindung wurde davon ausgegangen, dass der Schlüsseldatensatz im Speicher 3 der tragbaren Einheit 1 hinterlegt ist. Eine solche Hinterlegung kann beispielsweise werksseitig bei der Herstellung der tragbaren Einheit geschehen. Darüber hinaus ist in Figur 1 eine alternative Möglichkeit zur Bereitstellung eines Schlüsseldatensatzes im Speicher 3 durch gestrichelte Linien angedeutet. Diese Möglichkeit erfordert eine Eingabevorrichtung 50 an der tragbaren Einheit 1, über welche von einem Benutzer ein Schlüsseldatensatz eingegeben und im Speicher 3 abgespeichert werden kann.

Vorzugsweise handelt es sich bei der Eingabevorrichtung 50 um ein Lesegerät für biometrische Charakteristika, welches zusätzlich mit einer Verarbeitungssoftware zur Analyse von sensorisch erfassten biometrischen Daten ausgestattet ist. Lesegeräte für biometrische Charakteristika sind in großer Anzahl bekannt und brauchen daher vorliegend nicht im Einzelnen erläutert zu werden. Diesbezüglich verwendbare Technologien umfassen zum Beispiel:

- die Fingerabdruck-Analyse, welche nachfolgend als stellvertretendes Beispiel betrachtet wird;
- die Sprecher-Erkennung;
- 25 - die Abtastung der Retina (Netzhaut);
- die DNA-Analyse;
- die Analyse der Ohrmuschelform;
- die Analyse der Handform;
- eine maschinelle Verarbeitung der Unterschrift einschließlich
- 30 einer - Analyse von Schreibgeschwindigkeit und Druckwechseln.

Aus den biometrischen Charakteristika eines Benutzers kann die

Eingabevorrichtung 50 einen (weltweit eindeutigen) Schlüsseldatensatz ableiten, wobei sichergestellt ist, dass nur der berechtigte Nutzer diesen Schlüsseldatensatz besitzt bzw. eingeben kann.

Bei der Eingabevorrichtung könnte es sich auch um eine

- 5 Spracherkennungseinheit (im Gegensatz zu einer Sprecher-Erkennung) handeln, welche den Schlüsseldatensatz aus einer speziellen Spracheingabe des Benutzers generiert.

- Die Eingabe eines Schlüsseldatensatzes durch einen Benutzer befreit weiterhin von der Notwendigkeit, die sensitiven Daten dauerhaft im Speicher der tragbaren Einheit 1 bereitzuhalten. Der Schlüsseldatensatz kann nämlich jederzeit vom
- 10 Nutzer wieder in den Speicher 3 eingegeben werden, zum Beispiel durch eine erneute Fingerabdruck-Analyse. Die tragbare Einheit muss daher nicht mehr sicher verwahrt und vor unbefugtem Zugriff geschützt werden, sodass sie insbesondere als Zusatzfunktion in ein vorhandenes Gerät wie beispielsweise eine Fernbedienung, einen iPronto (Philips), ein Mobiltelefon mit Bluetooth- oder IrDA-Schnittstelle, ein USB-
- 15 Dongle oder dergleichen integriert werden kann. Voraussetzung ist dabei, dass der Heim-Schlüsseldatensatz aus Sicherheitsgründen aus der tragbaren Einheit 1 gelöscht wird, sobald er an ein Netzwerkgerät 2 übermittelt wurde oder sobald eine vorgegebene Zeitspanne von beispielsweise 30 Sekunden nach Eingabe des Schlüsseldatensatzes über die Eingabevorrichtung 50 verstrichen ist.

- 20 Mit Hilfe der Gästeeinheit 13 kann der Benutzer einem Gast Zugriff auf den PC 2 gewähren. Dazu begibt sich der Gast oder der Benutzer in die Nähe des PCs 2 und löst durch das Betätigen der Taste 15 eine Übertragung des durch den Schlüsselgenerator 14 erzeugten Gast-Schlüsseldatensatzes 17 aus.

- Der Gast-Schlüsseldatensatz 17 besteht aus einer Bitfolge mit
- 25 zusätzlichen Bits zur Übertragung weiterer Informationen. Die zusätzlichen Bits kennzeichnen den Schlüsseldatensatz als Gast-Schlüsseldatensatz und dienen zur Unterscheidung der Schlüsseldatensätze von anderen Informationen, falls die Empfangseinheit als Schnittstelle für weitere Anwendungen genutzt wird.

- Die Empfangseinheit 7 empfängt den Gast-Schlüsseldatensatz 17. Die
- 30 Empfängersoftware 11 identifiziert den Schlüsseldatensatz anhand der zusätzlichen Bits als Gast-Schlüsseldatensatz 17 und leitet den extrahierten Schlüssel als zusätzlichen (WEP-) Schlüssel über die Management-Schnittstelle an die Treibersoftware 10 der

Funkschnittstelle 12 weiter. Die Treibersoftware 10 verwendet den Schlüssel als zusätzlichen Schlüssel zur Verschlüsselung des Datenverkehrs.

In der im IEEE802.11 Standard definierten Wired Equivalent Privacy (WEP)-Verschlüsselung ist eine parallele Verwendung von bis zu vier WEP-Schlüsseln
5 vorgesehen. Die Geräte des Netzwerks sind in der Lage zu erkennen, welcher der WEP-Schlüssel aktuell zur Verschlüsselung verwendet wird.

Die Eingabe des Gast-Schlüsseldatensatzes 17 wird an allen Geräten des Hausnetzwerks wiederholt, die der Gast nutzen möchte, sowie an den Geräten des Gastes (z.B. Laptop), mit denen dieser Zugriff auf das Hausnetzwerk, z.B. auf die MP3-
10 Dateien auf PC 2, erhalten möchte.

Um dem Benutzer die Kontrolle über die Dauer des gewährten Gast-Zugangs zum Hausnetz zu ermöglichen, wird automatisch nach einer festgelegten Zeitspanne (z.B. 10h) oder durch Benutzer-Interaktion (z.B. Eingabe des Heim-Schlüsseldatensatzes 4 an den Hausnetz-Geräten) der Gast-Schlüsseldatensatz 17 in den
15 Geräten des Hausnetzwerks gelöscht.

Um eine unbefugte Benutzung eines Gast-Schlüsseldatensatzes durch einen früheren Gast zu verhindern, erzeugt der Schlüsselgenerator nach einer festgelegten Zeitspanne automatisch einen neuen Gast-Schlüsseldatensatz nach dem Zufallsprinzip.

20 Fig. 2 zeigt ein Blockschaltbild einer tragbaren Einheit 19 bei Verwendung einer Hochfrequenz-Transpondertechnologie zur Übertragung des Schlüsseldatensatzes 4. Die tragbare Einheit 19 besteht aus einem digitalen Teil 26, das einen Speicher 20 (wie z. B. ROM) zur Speicherung des Schlüsseldatensatzes, eine Ablaufsteuerung 21 und einen Modulator 22 zur Umsetzung eines aus der
25 Ablaufsteuerung 21 kommenden Bitstroms in zu übertragene Hochfrequenzsignale enthält. Weiterhin besteht die Einheit 19 aus einer Weiche 23 zur Trennung der durch ein als Antenne 25 bezeichnetes passives Bauelement empfangenen elektromagnetischen Energie von dem zu übertragenden Hochfrequenzsignal, einer Spannungsversorgungseinheit 24 mit Spannungsdetektor zur Versorgung des digitalen
30 Teils 26 mit einer Betriebsspannung und der Antenne 25 zur Übertragung des aus der Weiche 23 kommenden Bitstroms als auch zum Empfang der für den Betrieb notwendigen Energie.

Zur Übertragung des Schlüsseldatensatzes 4 begibt sich der Benutzer mit der tragbaren Einheit 19 in unmittelbare Nähe der Empfangseinheit 7. Die Antenne 25 leitet die einströmende Energie von der Empfangseinheit 7 über die Weiche 23 an die Spannungsversorgungseinheit 24 mit Spannungsdetektor weiter. Falls ein

5 Schwellenwert der Spannung in dem Spannungsdetektor überschritten wird, sorgt die Spannungsversorgungseinheit 24 für eine Betriebsspannung in der Einheit 19. Durch die Betriebsspannung angeregt wird die Ablaufsteuerung 21 initialisiert und liest den in dem Speicher 20 gespeicherten Schlüsseldatensatz aus. Der Schlüsseldatensatz wird durch die Ablaufsteuerung 21 in ein geeignetes Nachrichtenformat eingebettet und an

10 den Modulator 21 zur Umwandlung in analoge Hochfrequenzsignale weitergeleitet. Die Hochfrequenzsignale werden über die Weiche 23 durch die Antenne 25 ausgesendet.

In Fig. 3 ist die Einheit 19 als Empfangs- und Sendeeinheit bei Verwendung der gleichen Technologie wie in Fig. 2 dargestellt. In dieser Darstellung sind gleiche oder entsprechende Elemente und Komponenten wie in Fig. 2 jeweils mit

15 gleichen Bezugsziffern bezeichnet. Insoweit wird auf die Beschreibung im Zusammenhang mit Fig. 2 Bezug genommen, und nachfolgend werden nur die Unterschiede erläutert.

In dieser Ausführungsform weist die Einheit 19 neben dem Modulator 21 einen Demodulator 27 auf. Der Speicher 20 wird durch einen löschbaren Speicher wie

20 z.B. einen elektrisch löschbaren Speicher eines EEPROM realisiert.

Durch den Demodulator 27 ist die Einheit 19 in der Lage, ein durch die Antenne 25 (zusätzlich zur einströmenden Energie) empfangenes und über die Weiche 23 weitergeleitetes Hochfrequenzsignal in eine Bitfolge umzusetzen. Die vom Demodulator 27 kommende Bitfolge wird durch die Ablaufsteuerung 21 verarbeitet.

25 Die Verarbeitung der Bitfolge kann in einem Zugriff der Ablaufsteuerung 21 auf den Speicher 20 resultieren, falls die Ablaufsteuerung 21 feststellt, dass die Bitfolge Informationen enthält, die die Empfangseinheit zum Empfang des Schlüsseldatensatzes berechtigen. Falls die Empfangseinheit berechtigt ist, den Schlüsseldatensatz zu empfangen, liest die Ablaufsteuerung 21 den Schlüsseldatensatz aus und leitet ihn wie

30 in Fig. 2 beschrieben zur Aussendung an die Antenne 25 weiter.

Durch den Demodulator 27 ist es des weiteren möglich, einen neuen Schlüsseldatensatz in die Einheit 19 einzubringen. Wird der Speicher 20 als

beschreibbarer Speicher (z.B. EEPROM) realisiert, lässt sich auf diese Weise der in der Einheit 19 enthaltene Schlüsseldatensatz durch einen neuen Schlüsseldatensatz ersetzen.

In Fig. 4 ist die Einheit 19 als eine Gästeeinheit 28 bei Verwendung der gleichen Technologie wie in Fig. 2 dargestellt. In dieser Darstellung sind ebenfalls
5 gleiche oder entsprechende Elemente und Komponenten wie in Fig. 3 jeweils mit gleichen Bezugsziffern bezeichnet. Insoweit wird auf die Beschreibung im Zusammenhang mit Fig. 3 Bezug genommen, und nachfolgend werden nur die Unterschiede erläutert.

Die Gästeeinheit 28 weist zusätzlich einen Schlüsselgenerator 29 auf, der
10 mit der Ablaufsteuerung 21 verbunden ist und zur Erzeugung einer Folge von Gastschlüsseldatensätzen dient.

Nachdem die durch die Antenne 25 in unmittelbarer Nähe der Empfangseinheit 7 einströmende Energie in der Spannungsversorgungseinheit 24 mit Spannungsdetektor detektiert wurde, wird die digitale Einheit 26 durch die
15 Spannungsversorgungseinheit 24 mit einer Betriebsspannung versorgt. Die Ablaufsteuerung 21 liest einen durch den Schlüsselgenerator 29 erzeugten Schlüsseldatensatz ein. Nachdem die Ablaufsteuerung 21 den Schlüsseldatensatz erhalten hat und in ein geeignetes Nachrichtenformat eingebettet hat, leitet sie ihn weiter zur Versendung an den Modulator 22 und schreibt gleichzeitig den Schlüsselsatz
20 in den Speicher 20 ein, der für diesen Zweck als beschreibbarer Speicher ausgeführt sein muss (z.B. EEPROM).

In einer zweiten Betriebsart wird vom Schlüsselgenerator in regelmäßigen Abständen (zum Beispiel einige Minuten oder Stunden) ein neuer Schlüsseldatensatz erzeugt und im wiederbeschreibbaren Speicher 20 abgelegt. Der
25 weitere Ablauf entspricht dann den Erläuterungen wie zu Fig. 2 und Fig. 3 angegeben.

Die Ausführungsform der Einheit 19 mit Schlüsselgenerator wie in Fig. 4 gezeigt ist auch mit der in Fig. 2 gezeigten Ausführungsform (ohne Demodulator 27) kombinierbar.

PATENTANSPRÜCHE:

1. Sicherheitssystem für drahtlose Netzwerke mit einer ersten tragbaren Einheit (1) mit einem Speicher (3) zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes (4), die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4) vorgesehen ist, und
- 5 mindestens einer Empfangseinheit (7) in wenigstens einem drahtlosen Gerät (2) des Netzwerks, die einen Empfänger (9) zum Empfang des Schlüsseldatensatzes (4) und eine Auswertekomponente (11) des Gerätes zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes (4) oder eines Teils des Schlüsseldatensatzes in eine zweite Komponente aufweist.
- 10
2. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, dass der weltweit eindeutige Schlüsseldatensatz (4) im Speicher (3) der tragbaren Einheit (1) vom Hersteller vorgegeben wird.
- 15 3. Sicherheitssystem nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die tragbare Einheit (1) eine Eingabevorrichtung (50) zur Bereitstellung eines Schlüsseldatensatzes an den Speicher (3) enthält.
4. Sicherheitssystem nach Anspruch 3, dadurch gekennzeichnet,
- 20 dass die Eingabevorrichtung (50) dazu eingerichtet ist, biometrische Charakteristika eines Benutzers zu erfassen und hieraus einen Schlüsseldatensatz abzuleiten und/oder hiermit eine Authentifizierung des Benutzers vorzunehmen.

5. Sicherheitssystem nach Anspruch 3 oder 4, dadurch gekennzeichnet, dass die tragbare Einheit (1) dazu eingerichtet ist, einen mittels der Eingabevorrichtung (50) bereitgestellten Schlüsseldatensatz nach einer vorgegebenen Zeitdauer und/oder nach einer Verarbeitungsprozedur wieder aus dem Speicher (3) zu löschen.
- 5 6. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, dass die erste Einheit (1) eine Auslöseeinheit (5) zur Auslösung einer Kurzstreckenschlüsseldatensatzübertragung aufweist.
- 10 7. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, dass eine in der Einheit (1) enthaltene Detektoreinheit zur Auslösung der Kurzstreckeninformationsübertragung des Schlüsseldatensatzes (4) bei Annäherung an die Empfangseinheit (7) vorgesehen ist.
- 15 8. Sicherheitssystem nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass ein Schlüsselgenerator (14) in der ersten Einheit (1) oder einer zweiten Einheit (13) zur Erzeugung einer Folge von Gast-Schlüsseldatensätzen (17) vorgesehen ist.
- 20 9. Sicherheitssystem nach einem der Ansprüche 6 bis 8, dadurch gekennzeichnet, dass die erste Einheit (1) beim Betätigen einer zweiten Auslöseeinheit (15) zur Übertragung eines Gast-Schlüsseldatensatzes (17) vorgesehen ist.
10. Sicherheitssystem nach Anspruch 1 oder 9, dadurch gekennzeichnet, dass der Schlüsseldatensatz (4) und der Gast-Schlüsseldatensatz (17) jeweils aus einer Bitfolge bestehen.
- 25 11. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, dass die erste Einheit (1) ein Teil eines Gerätes, insbesondere einer Fernbedienung, ist.

12. Sicherheitssystem nach Anspruch 1, dadurch gekennzeichnet, dass eine Eingabe des Schlüsseldatensatzes (4) während oder vor einer Netzwerkkonfiguration, insbesondere einer automatischen Netzwerkkonfiguration, eines Gerätes (2) vorgesehen ist.

5

13. Sicherheitssystem nach Anspruch 10, dadurch gekennzeichnet, dass der Schlüsseldatensatz (4) und der Gast-Schlüsseldatensatz (17) Kennzeichnungsbits enthalten, die zur Unterscheidung zwischen Schlüsseldatensätzen (4, 17) und anderen Bitfolgen vorgesehen sind und die Bitfolgen als Schlüsseldatensatz (4) oder als Gast-Schlüsseldatensatz (17) kennzeichnen.

10

14. Sicherheitssystem nach Anspruch 8, dadurch gekennzeichnet, dass das Gerät (2) zur Löschung des Gast-Schlüsseldatensatzes (17) vorgesehen ist.

15

15. Sicherheitssystem nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass das Gerät (2) mittels eines im Schlüsseldatensatz (4,17) enthaltenen Schlüssels zur Authentifizierung und Verschlüsselung zu übertragener Nutzdaten zwischen den Geräten des Netzwerks vorgesehen ist.

20

16. Sicherheitssystem nach einem der Ansprüche 1 bis 14, dadurch gekennzeichnet, dass das Gerät (2) mittels eines im Schlüsseldatensatz (4,17) enthaltenen Schlüssels die Zugehörigkeit zu einem drahtlosen Netzwerk identifiziert.

25

17. Tragbare Einheit (1) zur Installation eines gemeinsamen Schlüssels in wenigstens einem Gerät (2) eines drahtlosen Netzwerkes mit einem Speicher zur Speicherung eines weltweit eindeutigen Schlüsseldatensatzes (4), die zur Kurzstreckeninformationsübertragung des Schlüsseldatensatzes vorgesehen ist.

30

18. Elektrisches Gerät (2) mit einer Empfangseinheit (7), die einen Empfänger (9) zum Empfang eines Schlüsseldatensatzes (4) und eine Auswertekomponente (11) des Gerätes (2) zur Speicherung, Verarbeitung und/oder Weiterleitung des Schlüsseldatensatzes oder eines Teils des Schlüsseldatensatzes in eine
- 5 zweite Komponente (10) aufweist.

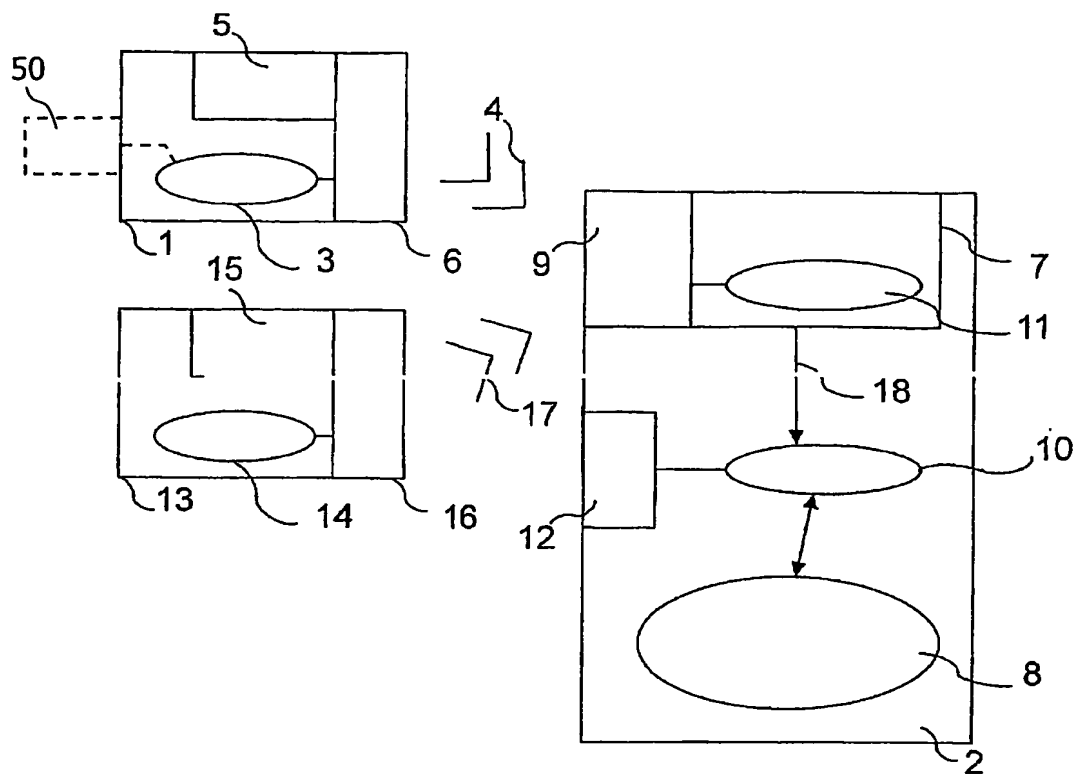


FIG. 1

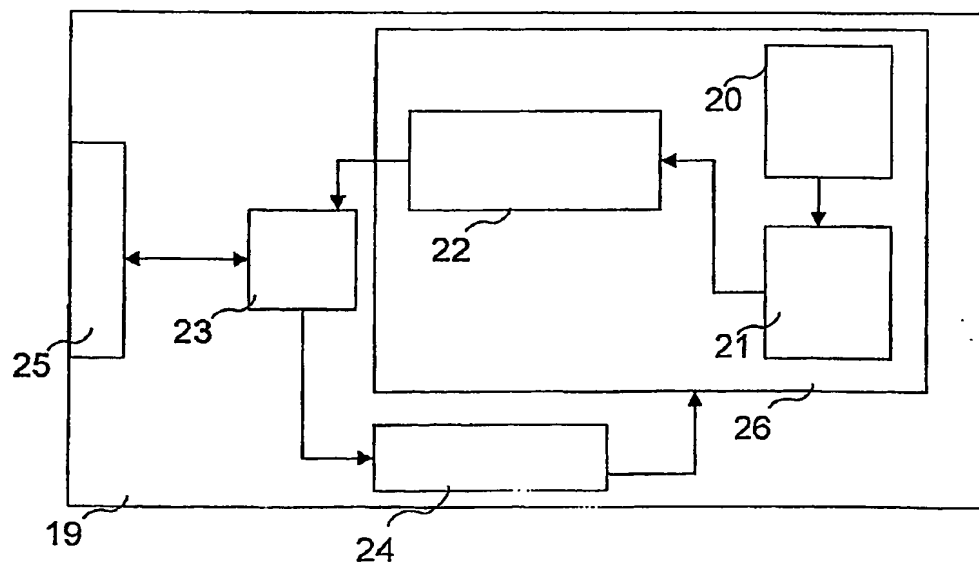


FIG. 2

2/2

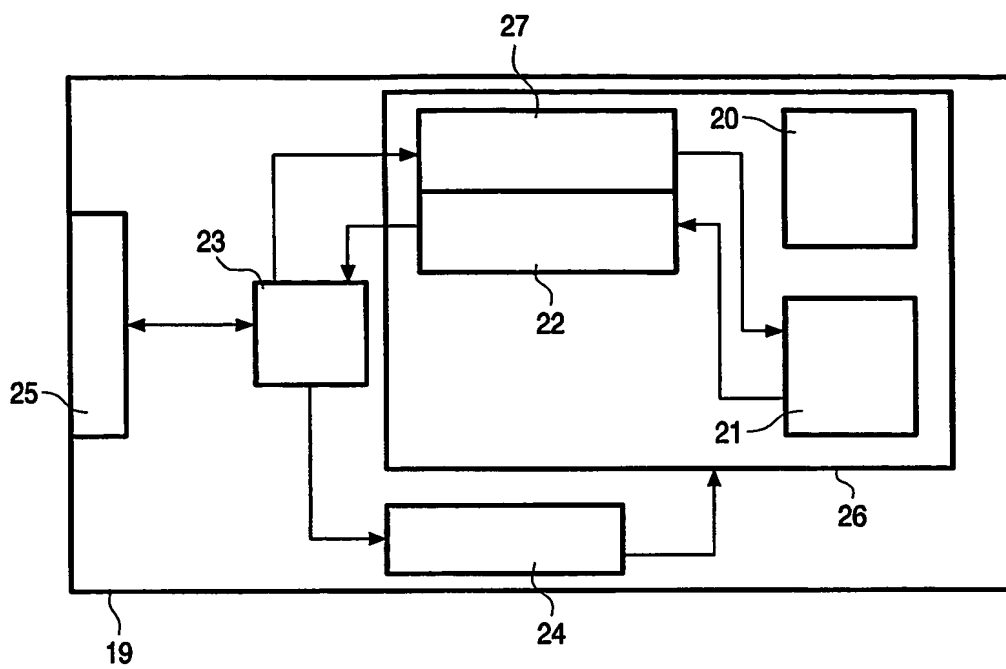


FIG. 3

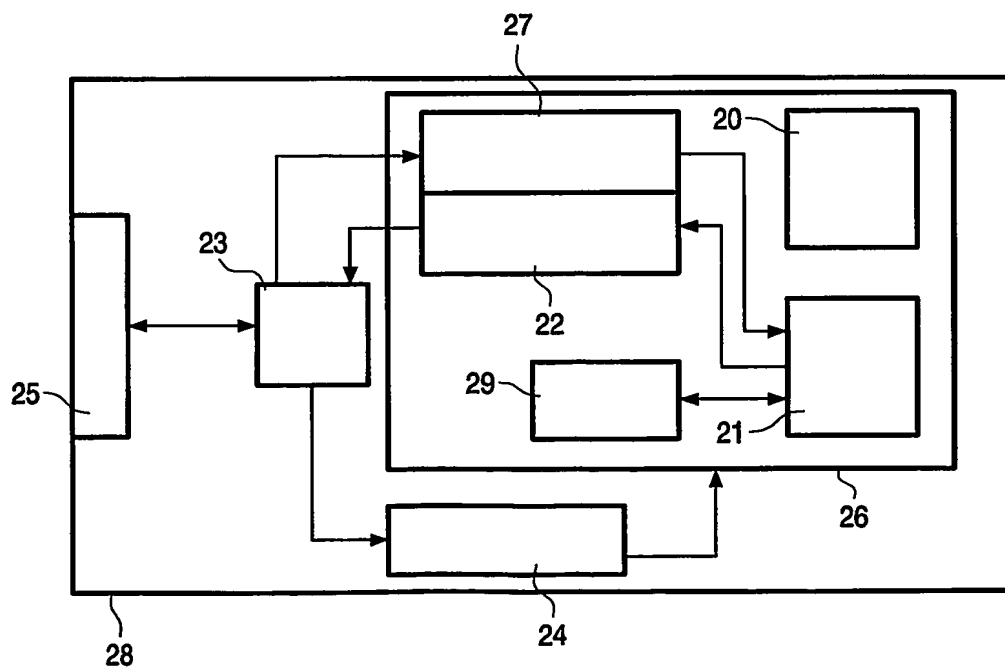


FIG. 4